UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/749,142	12/27/2000	Thomas Wille	DE000002	4761

65913	7590	09/05/2008

NXP, B.V.
NXP INTELLECTUAL PROPERTY DEPARTMENT
M/S41-SJ
1109 MCKAY DRIVE
SAN JOSE, CA 95131

EXAMINER
DINH, MINH

ART UNIT	PAPER NUMBER
2132	

NOTIFICATION DATE	DELIVERY MODE
09/05/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ip.department.us@nxp.com

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS,
WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _27 May 2008_.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _2-4 and 6-14_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _2,4 and 7-14_ is/are rejected.

7)☒ Claim(s) _3 and 6_ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _27 December 2000_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All   b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

Response to Amendment

1.   This office action is in response to the amendment filed 05/27/2008.

Response to Arguments

2.   Applicant's arguments with respect to the rejection of claims 2, 4, 7, 9 and 10-13

under 35 U.S.C. 103(a) as being unpatentable over Patarin et al. (6,658,569) in view of

Jahnich et al. (6,725,374) have been fully considered but they are not persuasive.

Patarin discloses a multiprocessor system having two or more processors for

performing cryptographic operations simultaneously and in parallel (Abstract; Fig. 2,

step A; col. 12, lines 6-12 and 31-40). Jahnich discloses using a dummy subprogram in

a cryptographic program and the execution of the dummy subprogram does not

influence the encryption result of the cryptographic program (col. 6, lines 29-52).

Applicant argues that the combination of Patarin and Jahnich would not produce the

method of claim 2 because neither Patarin nor Jahnich teaches or suggests the division

or segregation of useful operations from dummy operations, so that the useful

operations are performed with one processor and the dummy operations are performed

separately and independently (in parallel and simultaneously) with another processor

(page 5, last paragraph). However, it is fundamental in multiprocessor processing art

that parts of a program that do not depend on data generated by other parts are run in

parallel and simultaneously on different processors to achieve high performance. It is

clear that there is no data dependency between the dummy subprogram and the

cryptographic sub program(s); accordingly, they would be run in parallel and simultaneously on different processors.

Applicant argues that the combination of Patarin and Jahnich lacks proper motivation. Applicant reasons that because Jahnich teaches that useful and dummy operations should be "randomly distributed over time" to impede a DPA attack, anything else would be directly contrary to the teachings of Jahnich which explicitly advocates interspersing useful and dummy operation in time (page 6, last paragraph). Jahnich teaches utilizing dummy operations in a cryptographic program in different ways. Jahnich teaches that, in general, executing of dummy operations causes additional advantageous current fluctuations to be observed in a DPA analysis and thus contributes to the confusion of an attacker (col. 6, lines 28-38). Jahnich further teaches that it would provide additional benefits (i.e., to further impede a DPA attack) if the dummy operations are randomly distributed over time, i.e., they are not executed in a fixed order in relation to the useful operations (col. 6, lines 39-48). First, it is Jahnic's teaching of using dummy operations in general that is relied upon for the 103 rejection. Second, Jahnich's teaching that the dummy operations are not executed in a fixed order in relation to the useful operations in Jahnich's single-processor system does not exclude the dummy opeartion from being executed simultaneously with useful operations in a multiprocessor system.

Applicant argues that the combination would destroyed the princple of operation of the prior art invention being modified, i.e., Jahnich's (page 7, 3rd paragraph). It is Patarin's system that is modified, not Jahnich's.

Claim Rejections - 35 USC § 103

3.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

4.   Claims 2, 4, 7, 9 and 10-13 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Patarin et al. (6,658,569) in view of Jahnich et al. (6,725,374).

Regarding claims 2 and 10, Patarin discloses a device comprising a central

processing unit and one or more co-processors for performing cryptographic operations

simultaneously and in parallel (Abstract; Fig. 2, step A; col. 12, lines 6-12 and 31-40).

Patarin does not teach the use of dummy operations when performing a cryptographic

operation. Jahnich discloses using dummy operations, whose execution does not

influence an encryption result and that the consumption characteristics generated by the

dummy operation is part of the consumption characteristics of the smart card when

executing the cryptographic operation and the dummy operation so that reconstruction

of the consumption characteristics associated with performing the cryptographic

operation is impeded (col. 6, lines 29-52). It would have been obvious to one of

ordinary skill in the art at the time the invention was made modify the method of Patarin

to use dummy operations when performing a cryptographic operation, as taught by

Jahnich, so that reconstruction of the consumption characteristics associated with

performing the cryptographic operation would be impeded. Accordingly, the dummy

operation is performed in parallel and simultaneously with the cryptography operations

in Patarin's multiprocessor system because they do not depend on each other.

Regarding claims 4, 7, 11-13, Patarin further discloses that the cryptographic

operation is split up into at least two sub-operations and at least two processors perform

the sub-operations in parallel and simultaneously, while subsequently corresponding

sub-results are combined to an overall result of the overall cryptographic operation (Fig.

2; col. 12, lines 6-12 and 31-40).

5.   Claims 8 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Patarin in view of Jahnich as applied to claims 7 and 13 above, and further in view of

Tan (6,490,353). Patarin and Jahnich do not disclose that the split-up of the

cryptographic operation is randomly controlled. Tan discloses that data to be encrypted

is segmented into blocks and that the size of each data block and length of the

corresponding encryption key for each block are randomly selected (col. 3, lines 8-42);

the selection of the block size and the key length meet the limitation of splitting up a

cryptographic operation. It would have been obvious to one of ordinary skill in the art at

the time the invention was made modify the combined method of Patarin and Jahnich

such that the split-up of the cryptographic operation is randomly controlled, as taught by

Tan, to increase the degree of difficulty in attacking the encryption system.

Allowable Subject Matter

6.   Claims 3 and 6 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

7.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

        Mano, "Computer System Architecture"

8.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

        A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MINH DINH whose telephone number is (571)272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. D./
Examiner, Art Unit 2132

08/29/08

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132